STRATÉGIE DE SÉCURITÉ LOCALE DE WINDOWS

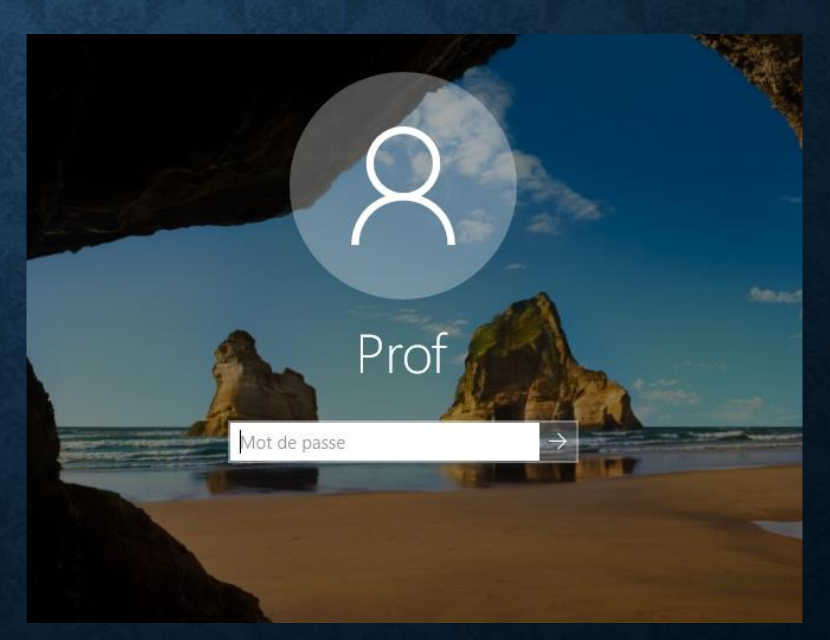
I- NOM D'UTILISATEUR ET MOT DE PASSE

Deux niveaux de protection par mot de passe sont recommandés :

- **BIOS** : empêche le système d'exploitation de démarrer et permet de rendre impossible la modification des paramètres du BIOS sans le bon mot de passe (illustration 1).



- **Ouverture de session** : empêche les accès non autorisés à l'ordinateur (illustration 2).



II- NOM D'UTILISATEUR ET MOT DE PASSE

- Les directives relatives aux **mots de passe** sont une composante importante d'une stratégie de sécurité.
- Un mot de passe doit être nécessaire pour qu'un utilisateur puisse accéder à un ordinateur ou se connecter à une ressource réseau.
- Les mots de passe permettent de **se protéger contre le vol de données et les autres actes malveillants.**
- Ils permettent également de **vérifier l'identité des utilisateurs**.

II – QU'EST-CE QU'UNE STRATÉGIE DE SÉCURITÉ ?

- Une **stratégie de sécurité** est un ensemble d'objectifs de sécurité qui garantissent la **sécurité du réseau, des données et des systèmes informatiques.**

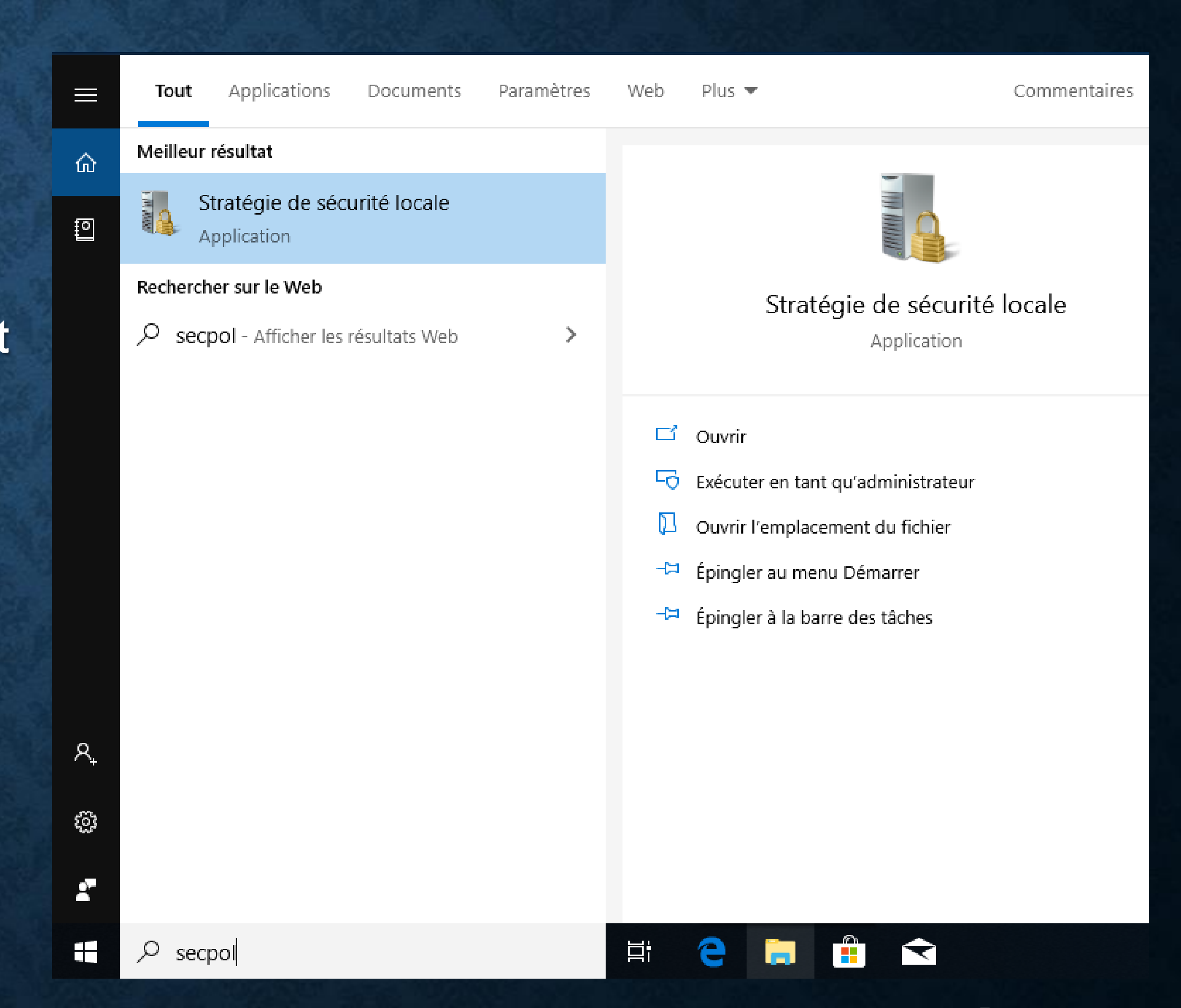
La stratégie de sécurité identifie…

- Quelles ressources doivent être protégées
- Quelles sont les menaces possibles
- Que faire si une faille est détectée
- Quelle formation est proposée aux utilisateurs

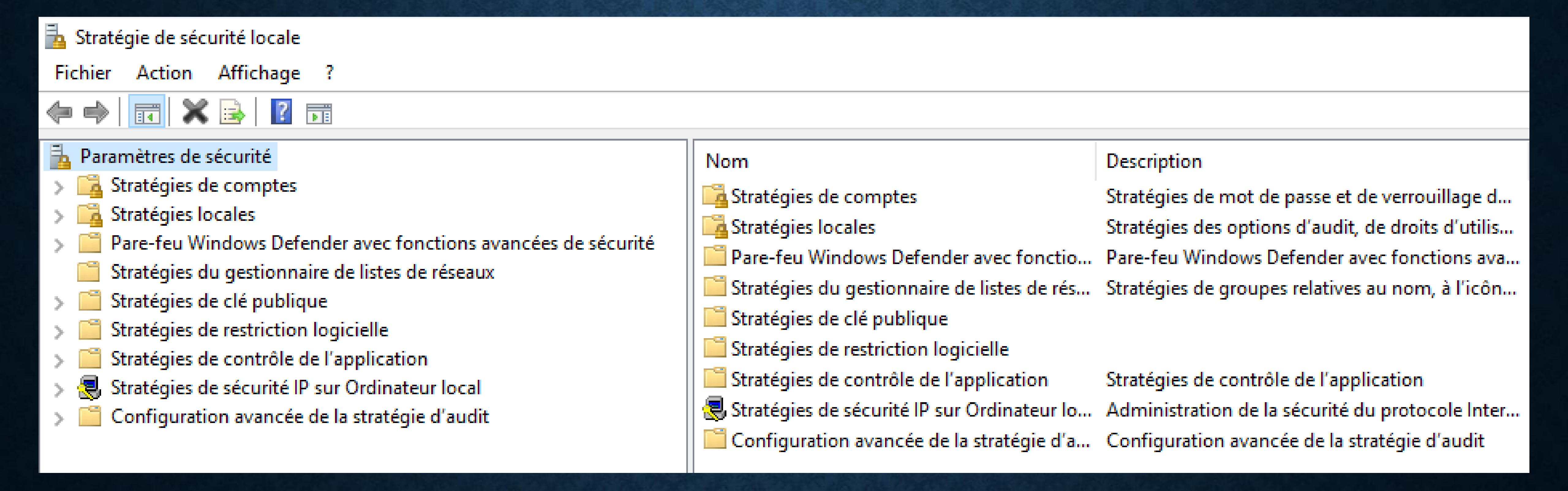


III- LA STRATÉGIE DE SÉCURITÉ LOCALE DE WINDOWS

- Sur la plupart des réseaux qui utilisent des ordinateurs Windows, **l'administrateur configure une stratégie de sécurité Locale.**
- Les stratégies de compte sont automatiquement définies **dès que l'utilisateur ouvre une session Windows.**
- Pour accéder à la Stratégie de sécurité locale dans Windows 10, procédez comme suit :
  - **Rechercher > secpol.**
- **L'outil Stratégie de sécurité locale** de Windows s'affiche, comme illustré ci-contre.



III- LA STRATÉGIE DE SÉCURITÉ LOCALE DE WINDOWS



IV- PARAMÈTRES DE STRATÉGIE DE COMPTE

- Lorsque vous attribuez des mots de passe, le niveau de contrôle doit correspondre au niveau de protection requis. Affectez autant que possible **des mots de passe forts**.
- L'illustration présente des **recommandations** pour la création de mots de passe forts.

Paramètres de sécurité
- Stratégies de comptes
  - Stratégie de mot de passe
  - Stratégie de verrouillage du comp
- Stratégies locales
- Pare-feu Windows Defender avec fon
- Stratégies du gestionnaire de listes de
- Stratégies de clé publique

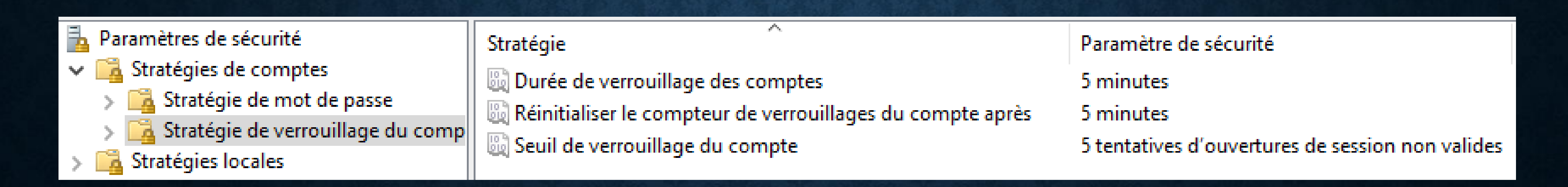
Stratégie	Paramètre de sécurité
Longueur minimale du mot de passe	8 caractère(s)
Le mot de passe doit respecter des exigences de complexité	Activé
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Durée de vie minimale du mot de passe	1 jours
Durée de vie maximale du mot de passe	90 jours
Conserver l'historique des mots de passe	24 mots de passe mémorisés

IV- PARAMÈTRES DE STRATÉGIE DE COMPTE

- **Longueur minimale du mot de passe** : le mot de passe doit contenir au moins 8 caractères.
- **Le mot de passe doit respecter des exigences de complexité** : le mot de passe ne doit pas contenir le nom du compte de l'utilisateur ni deux caractères consécutifs de son nom complet. Le mot de passe doit contenir trois des quatre catégories suivantes : lettres majuscules, lettres minuscules, chiffres et symboles.
- **Appliquer l'historique des mots de passe** : l'utilisateur peut réutiliser un mot de passe après avoir utilisé 24 mots de passe uniques.
- **Antériorité maximale du mot de passe** : l'utilisateur doit changer de mot de passe après 90 jours.
- **Antériorité minimale du mot de passe** : l'utilisateur doit attendre un jour avant de changer de mot de passe.

V- PARAMÈTRES DE STRATÉGIE DE VERROUILLAGE DE COMPTE

- Utilisez **Stratégie de verrouillage** pour empêcher toute tentative de connexion par force brute.
- Par exemple, la configuration de l'illustration permet à l'utilisateur d'entrer cinq fois un mauvais nom d'utilisateur ou mot de passe. Après **cinq tentatives**, le compte est verrouillé pendant **30 minutes**. Au bout de ces 30 minutes, le nombre de tentatives est remis à zéro et l'utilisateur peut à nouveau essayer d'ouvrir une session. Cette règle peut aussi **protéger contre les attaques par dictionnaire**, où chaque mot du dictionnaire est testé pour tenter d'accéder à l'ordinateur



VI- PARAMÈTRES DE SÉCURITÉ POUR LES STRATÉGIES LOCALES

- Certains paramètres dans **Options de sécurité** seront modifiés dans le laboratoire.
- Exemple: Les paramètres **Ouverture de session interactive**

Paramètres de sécurité
- Stratégies de comptes
  - Stratégie de mot de passe
  - Stratégie de verrouillage du comp
- Stratégies locales
  - Stratégie d'audit
  - Attribution des droits utilisateur
  - Options de sécurité
- Pare-feu Windows Defender avec fon
- Stratégies du gestionnaire de listes de

Stratégie	Paramètre de sécurité
Ouverture de session interactive : comportement lorsque la carte à puce est retirée	Aucune action
Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connecter	Votre activité est surveillée.
Ouverture de session interactive : ne pas afficher le nom de l'utilisateur lors de la connexion	Non défini
Ouverture de session interactive : ne pas afficher le nom du dernier utilisateur connecté	Désactivé
Ouverture de session interactive : ne pas demander la combinaison de touches Ctrl+Alt+Suppr.	Non défini
Ouverture de session interactive : nécessite l'authentification par le contrôleur de domaine pour le déverrouil...	Désactivé
Ouverture de session interactive : prévenir l'utilisateur qu'il doit changer son mot de passe avant qu'il n'expire	7 jours
Ouverture de session interactive : titre du message pour les utilisateurs essayant de se connecter	Attention:

VI- PARAMÈTRES DE SÉCURITÉ POUR LES STRATÉGIES LOCALES

- La plupart des paramètres de la section **Stratégies locales** de **Stratégie de sécurité locale** sortent du cadre de ce cours. Cependant, vous devez activer l'audit pour chaque **Stratégie d'audit**. Par exemple, sur l'illustration, l'audit est activé pour tous les **événements de connexion aux comptes**.

Paramètres de sécurité
- Stratégies de comptes
  - Stratégie de mot de passe
  - Stratégie de verrouillage du comp
- Stratégies locales
  - Stratégie d'audit
  - Attribution des droits utilisateur
  - Options de sécurité
- Pare-feu Windows Defender avec fon
- Stratégies du gestionnaire de listes de
- Stratégies de clé publique

Stratégie	Paramètre de sécurité
Auditer l'accès au service d'annuaire	Pas d'audit
Auditer l'accès aux objets	Pas d'audit
Auditer l'utilisation des privilèges	Pas d'audit
Auditer la gestion des comptes	Pas d'audit
Auditer le suivi des processus	Pas d'audit
Auditer les événements de connexion	Pas d'audit
Auditer les événements de connexion aux comptes	Réussite, Échec
Auditer les événements système	Pas d'audit
Auditer les modifications de stratégie	Pas d'audit

VII- OUTIL OBSERVATEUR D'ÉVÉNEMENTS

- L'Observateur d'événements tient un historique des événements concernant les applications, **la sécurité** et le système.
- Ces **fichiers journaux** constituent un outil de dépannage précieux, car ils fournissent les informations nécessaires à l'identification des problèmes.
- Pour accéder à l'Observateur d'événements de l'illustration , sélectionnez :

Panneau de configuration > Outils d'administration > Observateur d'événements

